DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY MATERIEL COMMAND
9301 CHAPEK ROAD, FORT BELVOIR, VA 22060-5527

AMC PAMPHLET NO. 25-36

12 May 2004

Information Management

OBTAINING A HEADQUARTERS ARMY MATERIEL COMMAND LOCAL AREA NETWORK ACCOUNT AND WORKSTATION

	Paragraph	Page
Purpose	1	1
Scope	2	1
References	3	2
APPENDIX A - Workflow Diagram		A-1
APPENDIX B - Government/Intern New Hire		B-1
APPENDIX C - Contractor New Hire		C-1
APPENDIX D - Foreign Representative		D-1
APPENDIX E – Waiver Process		E-1
APPENDIX F – Sample Templates:		
Notification to Pertinent Parties		F-1
Request for Equipment		F-2
Template of DOIM		F-3
Password Receipt Document		F-4
HQ AMC Information Assurance Awareness Policy Overview		F-5
APPENDIX G - Glossary of Terms		G-1
APPENDIX H - Determining Position Sensitivity and Position Designations		H-1

1. Purpose. This Pamphlet will provide written guidance, define responsibilities, and document the steps required to facilitate obtaining a Headquarters, Army Materiel Command (HQ AMC) Workstation and Local Area Network (LAN) Account.

2. Scope. This pamphlet has been developed to support U.S. HQ AMC personnel, to include Department of the Army Federal Employees, United States Military Personnel, HQ AMC Interns, HQ AMC Contractors and Foreign Representatives, working at the Army Materiel Command Headquarters facility located on Fort Belvoir, Virginia. At the time of publication, the DOIM personnel (DOIM COTR, DOIM IAM) are occupying the positions as identified

within this AMC Pamphlet may be contacted utilizing the following E-Mail Address: amcio-i@hqamc-exchg.army.mil.

3. References. Army Regulation (AR) 25-2, Information Assurance, Chapter 4, Section V: Personnel Security Standards

Army Regulation (AR) 380-67, Personnel Security Program

DOD Information Technology

AMC Control and Routing Slip, AMC Form 356-R-E

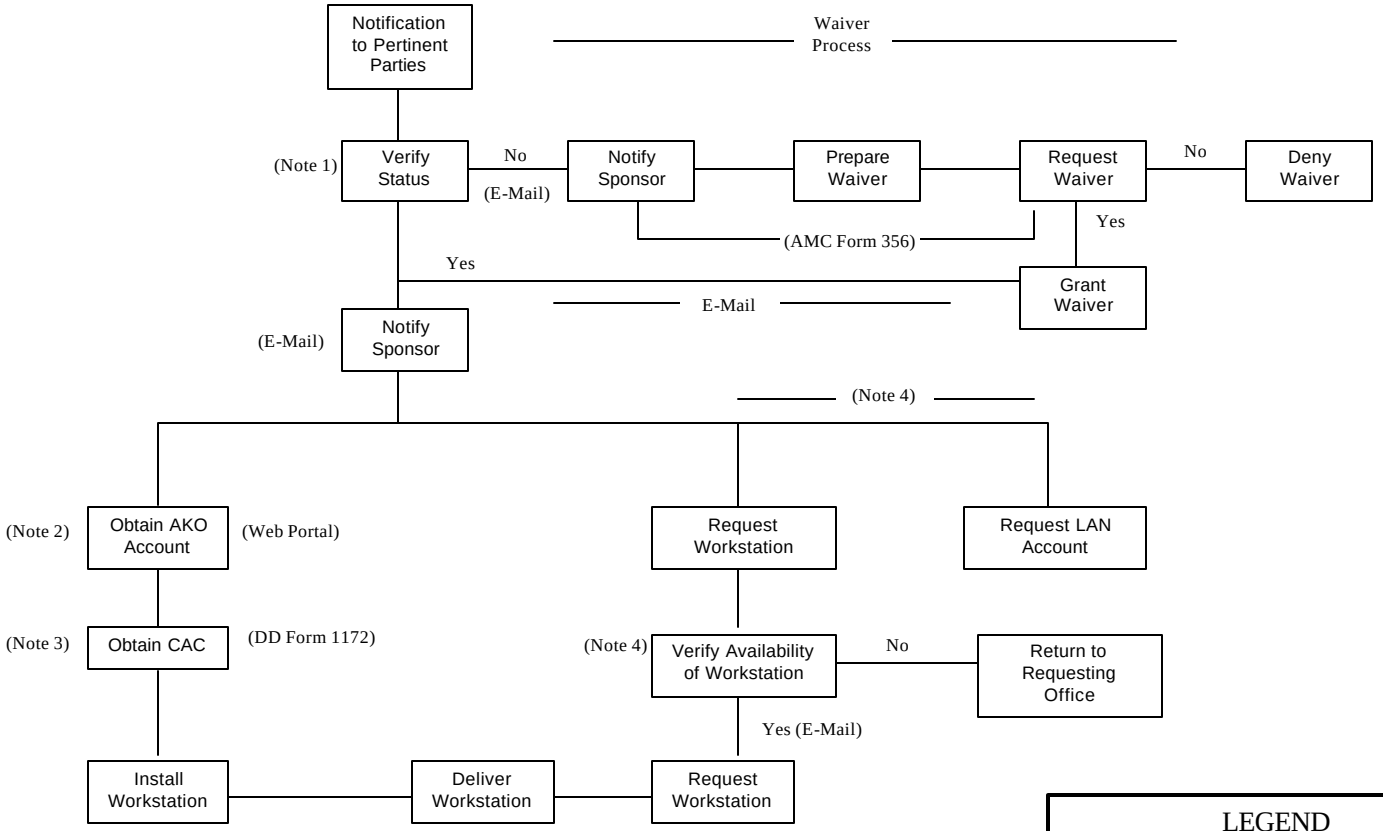
Application for Department of Defense Common Access Card DEERS E, DD Form 1172-2

The proponent of this regulation is the Chief Information Officer/G-6, Headquarters, U.S. Army Materiel Command. Users are invited to send comments and suggestions for improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Commander, U.S. Army Materiel Command, ATTN: AMCIO-P, 9301 Chapek Road, Fort Belvoir, VA 22060-5527

FOR THE COMMANDER:

RICHARD A. HACK
Lieutenant General, USA
Deputy Commanding General

Obtaining an HQ AMC LAN Account and Workstation



Note 1: Status – **Clearance Types**: Top Secret, Secret, Intern
Checks: NAC, NACI** Contractor Hire will have clearance identified as VAL
Note 2: New Hire must identify AMC Sponsor, AMC Sponsor must approve AKO Account Request
New Hire will require AKO Account for CAC
Note 3: AMC Sponsor must complete sec. 3 of DD Form 1172 for Gov't Hire/Intern
New Hire will require CAC to complete PKI Setup for Workstation
**Contractor New Hire must obtain Signature from COR
Note 4: Review/verify/approves Workstation availability against Seat Management Contract

LEGEND

AKO	Army Knowledge Online
AMC	Army Materiel Command
CAC	Command Access Card
COR	Contracting Officer's Representative
NAC	National Agency Check
NACI	National Agency Check w/Inquiries
PKI	Public Key Infrastructure
VAL	Visit Authorization Letter

Workflow Diagram

APPENDIX B

Government/Intern New Hire

Step 1. **AMC CPAC** notify Staff Section of new hire. The AMC CPAC (G-1, Personnel) provides Status of Personnel Security Investigation to Staff Section.

Status of Personnel Security Investigation: Completed Personnel Security Investigation: no additional work required, proceed with Step 2. If no suitable investigation results exist, process required Request for Waiver. (see: Appendix E, *Waiver Process*)

Step 2. **Staff Section** will notify (via E-Mail, digitally signed) all associated offices of new hire. (*see Appendix F, Notification to Pertinent Parties*)

Staff Section AMC Sponsor
Staff Section ITPOC/IASO
DOIM COTR

Step 3. **Staff Section AMC Sponsor** will identify to DOIM COTR requirements for Workstation/Laptop, to include non standard software. Request for Equipment should be submitted via E-Mail, digitally signed. (Microsoft Project, Microsoft VISIO…) (*see Appendix F, Request for Equipment*)

Step 4. **New Hire** utilizing Army Knowledge Online (AKO) Web Portal must request an AKO account. Preferred format is: fname.lname@us.army.mil. Access to AKO Web Portal will be provided by Staff Section AMC Sponsor. Staff Section AMC Sponsor may be required to sponsor New Hire AKO Account.

Step 5. **New Hire** will complete request for Common Access Card (CAC), DD Form 1172, Section 1. AMC in-line Approving Official Supervisor must sign and complete Section 3 to sponsor New Hire. New Hire is responsible for obtaining CAC from Military Personnel ID Card Office. (FormFlow Document: D1172_2.fro)

Step 6. **Staff Section ITPOC/IASO** requests from Directorate of Information Management (DOIM) ITPOC/IASO the creation of a LAN Account for New Hire. (via E-Mail, digitally signed)

Step 7. **DOIM ITPOC/IASO** based on requirements submitted by Staff Section AMC Sponsor (step 3) on behalf of New Hire submits a request for a Workstation to Help Desk (IT Helpdesk@hqamc-exchg.army.mil). (*see Appendix F, Template for DOIM*)

Step 8. **Help Desk** generates a helpdesk ticket which is assigned to the DOIM COTR.

Step 9. **DOIM COTR** reviews/verifies/approves/submits a request (Ticket) to Seat Management of new Workstation Requirement. Requests for Workstation which are denied are returned to the Staff Section AMC Sponsor and Staff Section ITPOC/IASO.

Step 10. **Seat Management** delivers and deploys new Workstation to New Hire. Deployment will require CAC Card and AKO to complete PKI Set-up. CAC is to be provided by New Hire with Personal Identification Number (PIN). Seat Management at time of deployment will PKI enable New Hire on assigned Workstation.

Step 11. **New Employee** signs Information Assurance Awareness Policy Overview in the presence of the DOIM ITPOC/IASO, retain for him/herself. *(see: Appendix F, Information Assurance Awareness Policy Overview)*

APPENDIX C

Contractor New Hire

Step 1. **Company** notifies Staff Section of new contractor hire. The contractor's employer must submit a Visitor Authorization Letter (VAL) to Staff Section. The VAL will identify the Clearance Status of the New Contractor Hire.

Status of Clearance: Valid Clearance: no additional work required, proceed with Step 2. If no suitable clearance exists, process required Request for Waiver. (see: Appendix E, *Waiver Process*)

Step 2. **Staff Section** will notify all associated offices of new hire. (*see Appendix F, Notification to Pertinent Parties*)

Staff Section AMC Sponsor (Gov't & Contractor Lead)
Staff Section ITPOC/IASO
DOIM COTR

Step 3. **Staff Section AMC Sponsor/Workload Manager** will identify to DOIM ITPOC/IASO requirements for Workstation/Laptop, to include non standard software. (Microsoft Project, Microsoft VISIO…) Request for Equipment is to be submitted, via E-Mail, digitally signed. (*see Appendix F, Request for Equipment*)

Step 4. **New Contractor Hire** utilizing AKO Web Portal must request an AKO account. Preferred format is: fname.lname@us.army.mil. Access to AKO Web Portal will be provided by Staff Section AMC Sponsor.

Step 5. **New Contractor Hire** will complete request for Common Access Card (CAC), DD Form 1172, Section 1. AMC Contracting Officer's Representative (COR) must sign and complete Section 3 to sponsor New Hire. New Contractor Hire is responsible for obtaining CAC from Military Personnel ID Card Office. (FormFlow Document: D1172_2.fro)

Step 6. **Staff Section ITPOC/IASO** requests from DOIM ITPOC/IASO the creation of a LAN Account for New Hire. (via E-Mail, digitally signed)

Step 7. **DOIM ITPOC/IASO** based on requirements submitted by AMC Sponsor on behalf of New Hire submits a request for a Workstation to Help Desk (IT Helpdesk@hqamc-exchg.army.mil). (s*ee Appendix F, Template for DOIM*)

Step 8. **Help Desk** generates a helpdesk ticket, which is assigned to the DOIM .

Step 9. **DOIM COTR** reviews/verifies/approves/submits a request (Ticket) to Seat Management for new Workstation Requirement. Requests for Workstation which are denied are returned to the AMC Sponsor and ITPOC/IASO.

Step 10. **Seat Management** delivers and deploys new workstation to new contractor hire. Deployment will require CAC Card and AKO to complete PKI Set-up. CAC is to be provided by new contractor hire with Personal Identification Number (PIN). Seat Management at time of deployment will PKI enable new contractor hire on assigned workstation.

Step 11. **New Contractor Hire** signs Information Assurance Awareness Policy Overview in the presence of the DOIM ITPOC/IASO, retain for him/herself. *(see Appendix F, Information Assurance Awareness Policy Overview)*

APPENDIX D

Foreign Representative Placement

Step 1. **Personnel** notify Staff Section of new Foreign Liaison Officer (LNO). The AMC CPAC provides Status of Personnel Security Investigation to Staff Section.

Status of Personnel Security Investigation: Completed Personnel Security Investigation: no additional work required, proceed with Step 2. If no suitable investigation results exist, process required Request for Waiver. (see: Appendix E, *Waiver Process*)

Step 2. **G-Staff** will notify all associated offices of new LNO. (*see Appendix F, Notification to Pertinent Parties)*

Staff Section AMC Sponsor
DOIM ITPOC/IASO
DOIM COTR

Step 3. **AMC Sponsor** (i.e., the LNO's Contact Officer (CO)) will identify to DOIM ITPOC/IASO requirements for Workstation/Laptop, to include non standard software. Request for Equipment should be submitted via E-Mail digitally signed. (Microsoft Project, Microsoft VISIO…) (*see Appendix F, Request for Equipment*)

Step 4. **New LNO** utilizing Army Knowledge Online (AKO) Web Portal must request a NIPRNET E-Mail account. Format for E-Mail address must be: lname.fname.MI.Foreign National.country name.program.host name.army.mil. In order to provide access to AKO, an exception to policy must be generated through G-6 channels to DA G-6 (DISC4) per AR 25-2. Format for E-Mail address will be the same as above, except "host name" will be "us." The AKO account must be sponsored. The sponsor should be the LNO's CO.

Step 5. **New LNO** will complete request for Common Access Card (CAC), DD Form 1172, Section 1. AMC in line Approving Official Supervisor must sign and complete Section 3 to sponsor New LNO. (FormFlow Document: D1172_2.fro)

Step 6. **Staff Section ITPOC/IASO** requests from Directorate of Information Management (DOIM) ITPOC/IASO the creation of a LAN Account for New Hire.

Step 7. **DOIM ITPOC/IASO** based on requirements submitted by Staff Section AMC Sponsor (Step 2) on behalf of New LNO submits a request for a Workstation to Help Desk (IT Helpdesk@hqamc-exchg.army.mil). (s*ee Appendix F, Template for DOIM*)

Step 8. **Help Desk** generates a helpdesk ticket which is assigned to the DOIM COTR.

Step 9. **DOIM COTR** reviews/verifies/approves/submits a request (Ticket) to Seat Management for new Workstation Requirement. Requests for Workstation which are denied are returned to the Staff Section AMC Sponsor and Staff Section ITPOC/IASO.

Step 10. **Seat Management** delivers and deploys new workstation to new LNO. Deployment will require CAC Card and AKO to complete PKI Set-up. As stated in Step 4, PKI cannot be implemented unless access to AKO has been approved by DA G-6.

Step 11. **New LNO** signs Information Assurance Awareness Policy Overview in the presence of the DOIM ITPOC/IASO, retain for him/herself. *(see Appendix F, Information Assurance Awareness Policy Overview)*

APPENDIX E

Waiver Process

Under the condition that the New Hire (Government/Intern/Contractor) does not have a valid or suitable Clearance, a Waiver must be requested in accordance with Army Regulation AR-25-2, Information Assurance, citation 4-16: Personnel Security Standards, and DOD Information Technology Security Accreditation Process (DITSCAP 5200.40, citation Appendix E, pg 11-14. To determine Clearance Level refer to Appendix H, Determining Position Sensitivity and IT Position Designations.

Valid Clearance Types:
- Top Secret
- Secret
- Interim

Background Checks:
- NAC/NACI
- Favorable Position of Trust (IT-III Only)

Step 1. **Staff Section** will notify (E-Mail, digitally signed) Staff Section AMC Sponsor and DOIM ITPOC/IASO of the Status of Security Clearance and the requirement for a Waiver.

Step 2. **Staff Section ITPOC/IASO** will prepare a Waiver Request utilizing AMC Form 356 and submit completed request to DOIM IAM. (FormFlow Document: Amc356.frp or AMC Form 356-R-E). The Request for Waiver must include;

Full Name: (last, first mi)
Company:
Duration of Waiver:
Status of Security Investigation:
System to which Access will be granted:
Justification of Waiver:

Step 3. **DOIM IAM** will submit Waiver Request to HQ-AMC DAA.

Step 4. **HQ-AMC DAA** will return Waiver Request (AMC Form 356) to DOIM IAM.
Waiver granted, return to In Process Step 2.
Waiver denied access to HQ-AMC Networks or LAN Account not authorized.

APPENDIX F

SAMPLE TEMPLATE

Notification to Pertinent Parties

To be completed by G-Staff and E-Mailed to appropriate offices/officers.

Identification	Last Name	First Name
Company/Country Name:	N/A for Government	
Scheduled Arrival Date		
Proposed Division:		
Seat Location/Cubical		

Staff Section or Separate Office must notify appropriate Office(s). Officials in each office may be different depending on originating office. Offices for G6 are as follows:

1. G-Staff ITPOC/IASO
2. DOIM COTR

Note: E-Mail correspondence must be Digitally Signed.

APPENDIX F

SAMPLE TEMPLATE

Request for Equipment

To be Completed by Staff Section AMC Sponsor or Workload Manager and E-Mailed to DOIM ITPOC/IASO

WorkStation	Specify	
	?	Desktop
	?	Laptop
	?	Docking Station
	?	Blackberry
Additional Software	Specify and write in any additional software requirements	
	?	Microsoft Project
	?	Microsoft VISIO
	?	
	?	
	?	
	?	
	?	
	?	
	?	

	Printed Name	**Signature**
Requesting Official		
DOIM Coordination		
Approving Official		

Note: E-Mail correspondence must be Digitally Signed.

APPENDIX F

SAMPLE TEMPLATE

Template of DOIM

To be completed by Staff Section ITPOC/IASO and E-Mailed to DOIM COTR

User Information
User Name:
Room No.:
Phone No.:
Office Symbol:
Contractor Name:
Required Completion Date:

Requested Action Information
Classification:
Unclassified: X Classified:
Account:
LAN: X
TSACS: only applicable if Laptop… LAN account is automatic on all PCs and Notebooks

New Equipment:
PC:
Laptop: n/a
Blackberry: n/a

Rebaselined Equipment:
PC: X
Laptop: n/a
Blackberry: n/a

Drop: ___ Installed (unclass) _X_ Activated (unclass) Drop No.: _____
___ Installed (class) ___ Activated (class) Drop No.: _____

Does user currently have a PKI Certificate? Yes/No
Does user have a requirement for issuance of PKI Certificate? Yes/No
Does user currently have a CAC card? Yes/No
Does user have a requirement for issuance of CAC card? Yes/No

Technical Information
IT Deployment Sheet No.:

Mail Groups: AMCIO-ALL-PERSONNEL;
Shared Drives:
Lotus Notes Databases:
Printers:
B/W: Room #
Color: Room #

Comment: This user is a new hire for a new position.

Thanks, *DOIM ITPOC/IASO signature, Telephone Number*

APPENDIX F

SAMPLE TEMPLATE

Headquarters Army Materiel Command (HQ AMC)

Information Assurance

Awareness Policy Overview

1. As an employee of the Federal Government, or Contractor and a user of government computer services, computer networks, and software, I understand my responsibilities to observe the policies set forth in AR 380-19, and any applicable HQ AMC Information Assurance (IA) directives.

2. Major policies and procedures include, but are not limited to:

a. Use of government computer services, networks, software, and hardware for official government work.

b. Will participate in an annual IA Security Training and Awareness program.

c. Process and store information ONLY on an accredited or approved system or workstation (i.e., approvals include sensitive but unclassified (SBU)).

DO NOT PROCESS CLASSIFIED INFORMATION VIA THE UNCLASSIFIED NETWORK (NIPRNET). ALL CLASSIFIED INFORMATION UP TO AND INCLUDING SECRET WILL BE PROCESSED VIA THE CLASSIFIED NETWORK (SIPRNET). CLASSIFIED INFORMATION DESIGNATED AS TOP SECRET OR HIGHER WILL BE PROCESSED VIA JWICS.

---

d. Protect all passwords and other authentication, identification codes and devices from unauthorized disclosure or release. Password aging is currently established at 90 days. The User will be prompted to change his/her password at a minimum of every 90 days.

e. Know the name of your activity Information Assurance Security Officer (IASO) and HQ AMC DOIM Information Assurance Manager (IAM).

f. If you have questions on information assurance (IA) or you do not understand IA policy/procedural statements, address your concerns with your IASO or contact the HQ AMC DOIM IAM.

g. Report all IA related incidents and/or violations to your IASO and the HQ AMC DOIM IAM.

h. Physically protect access to computer services, network, hardware and software from unauthorized personnel.

i. Obey all software copyright instructions and observe Federal copyright laws regarding the proper use and reproduction of software.

j. Ensure that you use the appropriate available protective measure for all information systems and networks.

k. Report all lost, missing or stolen hardware and software to your supervisor, IASO and the HQ AMC DOIM IAM.

l. Mark and label all removable media (floppy disk, zip disk, CD cartridge, etc.) to identify the content, classification or sensitivity of the information contained within.

m. Access the internet only to support official mission requirements and as authorized in paragraph 2-301, subparagraph (a) of the Department of Defense Directive (DODD) 5500.7.R DOD Joint Ethics Regulation ("Use of Federal Resources – Communication Systems").

n. Will not modify the system equipment or software, use it in any manner other than its intended purpose, introduce malicious software or code, or add user-configurable or unauthorized software (for example, instant messaging, peer-to-peer applications).

o. Establish a homepage on the internet only after approval and accreditation from the HQ AMC DOIM IAM, the Operation Security officer, Legal Counsel, and Public Affairs.

p. Avoid computer games, pornography, chain letters, unofficial business for personal use and other forms of behavior which is inappropriate and outside the scope of official government missions and functions as defined by applicable directives.

3. Report all virus incidents immediately to your IASO and seek assistance form the Help Desk.

4. I CERTIFY THAT I HAVE READ, ACKNOWLEDGED AND UNDERSTAND THE ABOVE.

PRINT USER NAME	SIGNATURE	OFFICE SYM	PHONE #	DATE
_____	_____	_____		_____
PRINT IASO NAME	SIGNATURE	OFFICE SYM	PHONE #	DATE
_____	_____	_____		_____

APPENDIX G

Glossary of Terms

AKO	Army Knowledge Online
AMC	Army Material Command
AMC Sponsor	Division Chief of AMC Directorate gaining New Hire
CAC	Common Access Card
CO	Contact Officer
COR	Contracting Officer's Representative
DAA	Designated Approving Authority (AMCIO)
Digitally Signed	PKI Signature, requires CAC
DOIM	Directorate of Information Management
DOIM COTR	Contracting Officer's Technical Representative, approving official for new Workstation, verifies availability against current Seat Contract
DOIM ITPOC/IASO	DOIM Information Technology Point of Contact/Information Assurance Security Officer
G-Staff	POC within AMC Directorate to which receives initial notification from G-1 of New Hire
G-Staff ITPOC/IASO	Information Technology Point of Contact within each AMC Directorate
HQ AMC DOIM IAM	Headquarters Army Material Command, Directorate of Information Management, Information Assurance Manager
IASO	Information Assurance Security Officer
IAM	Information Assurance Manager
ITPOC	Information Technology Point of Contact
LAN	Local Area Network
LNO	(Foreign) Liaison Officer
NAC	National Agency Check
NACI	National Agency Check with Inquiries
New Hire	New Employee, includes Civilian, Military, Intern, or Contractor
PIN	Personal Identification Number, utilized as a part of PKI
PKI	Public Key Infrastructure
POC	Point of Contact
Seat Management	Contractor supporting HQ AMC with Workstations, LAN, and Help Desk
Workload Manager	Senior POC for New Contractor Hire on site
VAL	Visit Authorization Letter
Web Portal	AKO Web-Page

APPENDIX H

Determining Position Sensitivity and IT Position Designations

1. Reference:

a. AR 25-2, Information Assurance.

b. AR 380-67, Personnel Security Program.

2. AR 25-2, paragraph 4-14a, identifies the requirement to designate positions requiring access to and processing of information on IT systems. This designation is one determining factor in the type of Personnel Security Investigation is required. The IT designations are:

a. IT-I. Personnel in these positions have privileged-level access to control, manage, or configure IA tools or devices, PCs, networks, and enclaves. These individuals may be network administrators, system administrators, or directors for information management. An individual assigned to an IT-I position will have their position sensitivity designated as critical sensitive, under AR 380-67, and will require the appropriate investigation for a critical sensitive position.

b. IT-II. Personnel in these positions have limited privileged-level access to control, manage, or configure ITs and devices. These individuals may be back-up operators or system administrators of common applications. Individuals with IT-II duties will be supervised by an individual designated as IT-I. The position sensitivity of an individual performing IT-II duties will be non-critical sensitive. Investigation requirements in AR 380-67 apply.

c. IT-III. All individuals accessing IT systems with non-privileged level access are considered to be performing IT-III duties. These individuals are common users who do not possess system level access. The position sensitivity for an individual performing IT-III duties will be nonsensitive. Investigation requirements in AR 380-67 also apply.

3. IT designations must not be confused with position sensitivity designations. The IT designation is one determining factor in the investigation process. AR 380-67 requires any individual assigned to a position designated as critical sensitive to submit the appropriate security forms as required to obtain a Top Secret clearance. The same requirement applies to the other two designations; an investigation required to obtain a Secret clearance on any individual assigned to an IT-II and a NAC/NACI for individuals assigned to an IT-III position. If an individual is selected for an IT-I or IT-II position and will not have access to any classified information, the appropriate investigation is still required, though a security clearance need not be provided. Likewise, if an individual is performing IT-III duties, but his/her responsibilities require access to classified information, then the more stringent investigation must take place. Therefore, even though the IT-III designation applies, the position must be designated as either critical sensitive (TS access) or non-critical sensitive (Secret access).